Title: Effecting IT Infrastructure Culture Change: Management by Processes and Metrics

Speaker: Robert L. Miller, Ph.D., JPL Information Technology Security Implementation Manager, Jet Propulsion Laboratory, California Institute of Technology

The ongoing transition of the United States economy from processing paper to electronic transactions has ushered in major productivity increases. Increasingly, companies are recognizing the strategic importance of managing their information technology (IT) assets, including communication networks and proprietary data. Consequently, many IT projects are now receiving executive management attention, since they address core business processes whose outcome can affect employees, customers, suppliers and possibly the organization's ability to survive in a competitive electronic marketplace.

The extent that government and business depend on information technology (IT) was not widely appreciated until preparations began to meet the Year 2000 (Y2k) threat. The Y2k threat required businesses to create detailed lists of their IT assets and then make quick decisions about how to handle each asset (fix, replace, or retire).

The Y2k threat is no longer in the headlines —it has been replaced by widely publicized attacks on IT security, such as denial-of-service and e-mail viruses. On the surface, the Y2k and IT security threats appear to be quite different, the former resulting from unanticipated design limitations, while the latter arising from intentional attacks. However, they both stem from IT infrastructure vulnerabilities. Addressing these vulnerabilities company-wide requires changing the culture of the IT infrastructure users. No longer can an employee consider company-owned IT assets to be "my computer", "my software", or "my network".

This talk describes the processes and metrics used by Jet Propulsion Laboratory to bring about the required IT infrastructure culture change to update and certify, as Y2k compliant, thousands of computers and millions of lines of code. It also addresses the application of this approach to IT security planning and implementation.